Final Report

Title: Quantum Algorithms and Initialization

Principal Investigator(s): Dong Pyo Chi, Prof.

Contract Number: FA5209-04-P-0228

AFOSR/AOARD Reference Number: AOARD-04-4003

AFOSR/AOARD Program Manager: Tae-Woo Park, Ph.D.

Period of Performance: 24 March 2004 – 23 March 2006

Submission Date: 31 August 2006

PI: Dong Pyo Chi, Prof.
School of Mathematical Science
Seoul National University
Seoul 151-742, Korea

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **11 SEP 2006**	2. REPORT TYPE **Final Report (Technical)**	3. DATES COVERED **24-03-2004 to 23-03-2006**

4. TITLE AND SUBTITLE **Quantum Algorithms and Initialization (QA&I)**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Dong Pyo Chi**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Seoul National Universiy,San 56-1, Shillim-dong, Kwanak-gu,Seoul 151-742,Korea (South),KE,151-742**	8. PERFORMING ORGANIZATION REPORT NUMBER **AOARD-044003**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) **The US Resarch Labolatory, AOARD/AFOSR, Unit 45002, APO, AP, 96337-5002**	10. SPONSOR/MONITOR'S ACRONYM(S) **AOARD/AFOSR**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

We are going to show that ?whether or not a function is evenly distributed? can be determined in quantum polynomial time without initialization. We will also show that the functional evaluation oracle and the functional phase transform are equivalent. To solve the first conjecture, we will construct a quantum algorithm to solve the reduced problem to determine ?whether or not a function is evenly balanced? and then extend this result by employing our initialization-free quantum functional evaluation oracle. For the second conjecture, we will construct the quantum functional evaluation oracle from the quantum functional phase transform. For this purpose, we will localize the both operators on the auxiliary register and then build a quantum circuit that can transform both localized operators to each other. We will extend the domain of the functional phase transform to the Hilbert space, which is the domain of a function evaluation oracle, so that the relative phase changes in the functional phase transform can be encoded into the control register. The limitation on the size of quantum computers makes it important to reuse qubits for auxiliary registers. Our initialization-free algorithm will greatly reduce the size of quantum computers since independent computational processes can share auxiliary registers. Furthermore, our algorithm can be useful in symmetric cryptography, because to design secure block ciphers it is essential to find evenly distributed functions. Moreover, until now it is not known how to implement functional evaluation on a quantum computer. Also which one is easy or possible to implement on a quantum computer among the functional phase transform and the functional evaluation oracle has not been answered yet. Thus our result can give a flexibility to the realization of functional evaluation on quantum computers.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES **19**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

Index

1. Objectives

Objective 1 : ***To construct a quantum algorithm to determine "Whether or not a function is evenly distributed" in quantum polynomial time without initialization*.**

A function $f : Z_N \to Z_M$ is called ***evenly distributed*** if it is many-to-one and onto an evenly spaced range. In more detail, the domain of f , Z_N is mapped onto a subset of K of Z_M which is evenly spaced elements in the range Z_M with constant separation M / K , where $K \leq M, N$.
We construct quantum algorithms which can determine whether or not a function is evenly distributed efficiently without initialization of the auxiliary register which is usually needed in quantum computational algorithms.

Objective 2 : ***"The functional evaluation oracle" can be constructed from the functional phase transform*.**

On a quantum computer, a function $f : Z_N \to Z_M$ is evaluated by ***the function evaluation oracle*** that computes $| x\rangle + | y\rangle \to | x\rangle + | y \oplus f(x)\rangle$, where the first quantum register is called the control register and the second register is called the auxiliary or ancillary register.
It has been shown that the quantum functional phase transform can be constructed from the quantum functional evaluation oracle without initialization of auxiliary registers. However, the converse has not been proven yet.
Objective 2 is to show the converse of the previous result. That is. The function evaluation oracle can be shown to be constructed from the functional phase transform that changes the phase of each qubit selectively.

2. Status of Effort

It was not so trivial to construct unitary operations by which the interference pattern on the phases for both evenly distributed functions and the others. So it was somewhat needed to restrict the domain of evenly-distribution functions to Z_2 (that is, Boolean functions) and to analyze the n-th root of unity produced by the quantum Fourier transform. Furthermore, we also simplified the problem of evenly-distribution function to be the problem of ***evenly balanced function*** on which we have constructed a quantum algorithm which can solve the problem in polynomial time. Based on this result we have constructed an initialization-free quantum algorithm that can determine "whether a function is evenly balanced or not" in quantum polynomial time. Then we have extended the range of the function in order to make it to be an evenly distributed one.

3. Abstract

We generalized quantum algorithm distinguishes a wider class of functions promised to be either constant or many to one and onto an evenly spaced range, so-called a ***evenly-distributed function***. As the original DJ-algorithm, the generalized algorithm solves this problem using a single functional evaluation.
In spite of the incredible computing power of quantum computer, it has been demanded to use a certain number of quantum registers in a specific state and the extra operations to initialize the state

of the registers. However, it would help a lot to reduce the storage and operations if one can use ***any arbitrary unknown quantum state*** that might be in the process of other quantum computer in order to operate one's own. So we consider the problem of distinguishing constant and evenly balanced functions and present a quantum algorithm for this problem that does not require any initialization of an auxiliary register involved in the process of functional evaluation and after solving the problem recovers the initial state of an auxiliary register. Based on this approach, we have investigated and present some algorithmic technique, in which a single auxiliary register in an arbitrary unknown state is sufficient to implement the iterative procedure that is usually necessary in quantum computations and recover the auxiliary register untouched. The technique is applicable to the most case of quantum algorithms that give us an exponential speed-up and ***this is far beyond our original objectives***. The new algorithmic technique can be applied to any case of hidden subgroup problems if the based group is commutative or not including period finding and Simon problems. Since most known applications of the QFT can be considered as a generalization of finding unknown period of a periodic function(for example, Shor's factoring algorithm[1] and Hallgren's more recent algorithm for solving Pell's equation)[2], the initialization-free technique could be applied to a lot of implementations of quantum algorithms.

3.1 Research Accomplishments

The Initialization-free generalized Deutsch-Jozsa type quantum Algorithms

We generalized the well-known Deutsch-Jozsa (DJ)[3] problem to the tasks of distinguishing between constant functions and so-called evenly distributed and evenly balanced functions, respectively. While any classical, deterministic black-box algorithm for the generalizations requires exponentially many function calls in the input length, the quantum algorithms we present here only need one or two such calls. The quantum circuit for the problem with evenly balanced function does not even require its auxiliary registers to be initialized.

We first briefly recall the original DJ problem [3]. The input is a function $f: Z_2^n \rightarrow Z_2$ computed by a black-box which is guaranteed to fulfill the following promise.
'Either f is a constant function, (i.e., $f(x)=0$ for all x or $f(x)=1$ for all x), or f is balanced, (i.e., $f(x)=1$ for exactly half of the inputs)'. Deutsch and Jozsa showed that this promise problem is solvable by a quantum circuit using only one invocation of a black-box for f, which carries out the unitary transformation

$$|x\rangle\otimes|y\rangle \xrightarrow{U_f} |x\rangle\otimes|y\oplus f(x)\rangle\ ,$$

where $x\in Z_2^n$ and $y\in Z_2$.

The whole circuit realizes the sequence of transformations

$$|0^n\rangle\otimes|0\rangle \xrightarrow{H^{\otimes(n+1)}} H^{\otimes n}|0\rangle\otimes H|0\rangle$$

$$\xrightarrow{U_f} \frac{1}{2^{n/2}}\sum_{x\in Z_2^n}(-1)^{f(x)}|x\rangle\otimes H|0\rangle$$

$$\xrightarrow{H^{\otimes n}} \frac{1}{2^n}\sum_{y\in Z_2^n}\sum_{x\in Z_2^n}(-1)^{x\cdot y+f(x)}|x\rangle\otimes H|0\rangle\ .$$

Where H is the *Hadamard transform* on a single qubit, $|0^n\rangle$ denotes the all-zero vector of length n, and $x\cdot y$ is the inner product of the vectors x and y on Z_2^n. The circuit requires an n-qubit register containing the input for f and one auxiliary qubit for the function value. The measurement of the n-qubit register after carrying out the above transformation yields $|0^n\rangle$ with certainty if the function is constant and some other vector if it is balanced.

The two generalizations of the DJ problem considered here are as follows.

(1) Problem GDJ-ED (generalized Deutsch-Jozsa for evenly distributed functions).
The input is a function $f: Z_N \to Z_M$ which is either constant or evenly distributed,
i.e.) There is an integer K dividing M and N and another integer t such that
(i) The image of f is equal to $(M/N)j+t \quad j=0,\ldots,K-1$
(ii) The function is (N/K)-to-one

(2) Problem GDJ-EB (generalized Deutsch-Jozsa problem for evenly balanced functions).
The input is a function $f: Z_N \to Z_M$ which is either constant or evenly balanced,
i.e.) For half of all output values y of f, the parity of all bits in the representation of y as a vector over Z_2^m, $m=[\log M]$, is equal to 1.

From now on, we assume for simplicity that $N=2^n$ and $M=2^m$. We may identify values from Z_N and Z_M with vectors from Z_2^n and Z_2^m.

We first discuss the quantum algorithm which can solve the problem GDJ-ED efficiently.
Note that the original DJ algorithm encodes the values of f into a sum of powers of -1, which is a square root of unity in Z_2 and this sum finally appears in the amplitude of $|0^n\rangle$. Then due to the properties of the roots of unity, the sum cancels out if the function under consideration is balanced. The idea in the algorithm for GDJ-ED is to compute a sum of M-th roots of unity over Z_M instead of a square root of unity in Z_2. Instead of the standard black-box in the original DJ algorithm, a black-box computing the transformation

$$|x\rangle \xrightarrow{U'_f} \omega^{f(x)}|x\rangle$$

is used, where $\omega := e^{2\pi i/M}$. This black-box operation is again sandwiched into two applications of the *Hadamard transform* on n-qubits, as in the original DJ-problem. The final state computed by the new algorithm is given by

$$\frac{1}{2^n}\sum_{y\in Z_2^n}\sum_{x\in Z_2^n}(-1)^{x\cdot y}\omega^{f(x)}|y\rangle .$$

For a constant function f, the amplitude of $|0^n\rangle$ in this sum is $\omega^{f(0)}$, i.e., the result is observed with certainty in a measurement of the n-qubit register. Due to the properties of the roots of unity, the amplitude is equal to 0 if f is evenly distributed, and thus, a result different from $|0^n\rangle$ is observed. Altogether, the algorithm solves the problem GDJ-ED.
Here, we present another algorithm which works with a black-box analogous to the standard one, realizing the transformation

$$|x\rangle \otimes |y\rangle \xrightarrow{U_f''} |x\rangle \otimes |y + f(x)\rangle$$

where $x \in Z_N$, $y \in Z_M$ and '+' stands for the addition modulo M .
This second algorithm requires an auxiliary register of $[\log M]$-qubits which is initialized with the all-ones vector, $|1^{\otimes[\log M]}\rangle$. It also needs to apply the black-box only once.

Now, we consider the quantum algorithm which can solve the problem GDJ-EB using any arbitrary mixed quantum state as the auxiliary register and recovering it at the end of algorithm without any deformation. The algorithm uses an n-qubit register initialized by $|0^n\rangle$ and an m-qubit auxiliary register which is assumed to be in an arbitrary pure state $|\Psi\rangle$. On these registers, the algorithm carries out the sequence of transformations

$$H^{\otimes n} \otimes I_m ,\ U_f^{\oplus} ,\ I_n \otimes \sigma_z^{\otimes m} ,\ U_f^{\oplus} ,\ \ I_n \otimes \sigma_Z^{\otimes m} , H^{\otimes n} \otimes I_m$$

in this order, where I_j denotes the identity operation on j qubits and

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The black-box operation $U_f^{\oplus}$ on $n + m$ qubits is defined as

$$|x\rangle \otimes |y\rangle \rightarrow |x\rangle \otimes |y \oplus f(x)\rangle$$

where $x \in Z_2^n$ and $y \in Z_2^m$ and '$\oplus$' denotes the bitwise exclusive-or, i.e., the addition in Z_2^m .
Then it can be shown that the final state obtained by these transformations is

$$\frac{1}{2^n} \sum_{y \in Z_2^n} \sum_{x \in Z_2^n} (-1)^{x \cdot y + p \circ f(x)} |x\rangle \otimes |\Psi\rangle$$

where $p : Z_2^m \rightarrow Z_2$ means the 'parity function', i.e., $p((x_1, \ldots, x_m)) = x_1 + \ldots + x_m \pmod 2$ for any $(x_1, \ldots, x_m) \in Z_2^m$.
Similarly with the original DJ-problem, constant and evenly balanced functions can now be distinguished by a measurement of the first n-qubits. Furthermore, in terms of 'purification', the algorithm also works for arbitrary initial states (i.e., also mixed ones) in the auxiliary register.

The Initialization-free quantum Algorithms for finding hidden subgroup structure (Simon problem and finding unknown period)

We have constructed a quantum algorithm that can solve Simon's problem[4] in polynomial times with allowing any arbitrary impure or even the completely mixed state $I/_{2n}$ as the auxiliary register and turn it back without any deformation . The cost of the algorithm is essentially one extra evaluation of U_f within the circuit and the ability to choose random classical bit-strings on each run. Moreover, replacing the *Hadamard* transforms in the algorithm for Simon's problem with *Quantum Fourier Transforms* (QFTs), it is also possible to similarly modify the usual quantum period-finding algorithm [1] to exploit fully mixed auxiliary registers.

A brief description of the algorithms is following.

First, we note that there exists an exact quantum polynomial-time algorithm for the Simon problem**[5]**. However, we here deal with the original Simon algorithm which is polynomial-time in the expected sense.

For convenience, we use the following notations. Let $G=\{Z_2^n,\oplus\}$ be a group under the binary operation $\oplus$, which is the bitwise **XOR** operation. For a subset $|A|$ of $|G|$, let $|A|$ denote the cardinality of A.

We define a bilinear map $G\times G\to Z_2$ such that

$$xy=x_0y_0\oplus\cdots\oplus x_{n-1}y_{n-1}\quad\text{with}\quad x=(x_0,\cdots,x_{n-1})\,,\,y=(y_0,\cdots,y_{n-1})$$

For a subgroup H of G, let $H^+=\{\ x\in G\,|\,xh=0\quad for\quad all\quad h\in H\ \}$ denote the orthogonal subgroup of H.

We remark that the quotient group ***G/H*** is well-defined since G is an abelian group.

Let $f:G\to G$ be an arbitrary two-to-one map such that *f*(x) = *f*(y) if and only if $x\oplus y\in H$ where *H* = {0, h} is a subgroup of G for some non-zero h in G. Then the Simon problem is to find the subgroup H, that is, to determine the value of h.

The original Simon algorithm is as follows:

(i) Prepare $\left|o^{\otimes n}\right\rangle\otimes\left|o^{\otimes n}\right\rangle$, (ii) Apply $W_n\otimes I$, where W_n is the n-qubit Walsh-Hadamard transform, (iii) Apply U_f, (iv) Apply $W_n\otimes I$.

Then the resulting state is $|\Phi\rangle=\frac{2}{G}\sum_{y\in H}\ \sum_{x'\in G/H}(-1)^{xy}|y\rangle\otimes|f(x)\rangle$. If we measure the first n-qubit state, then for each $y\in H^+$, the probability with which we obtain y as the outcome is $\frac{2}{|G|}$.

Thus, after expected ***O***(*n*) repetitions of this procedure, at least n linearly independent values of y can be collected so that the nontrivial h' is uniquely determined by solving the linear system of equations *h' y=0* and thus we have *h'=h* as required.

Now the initialization-free quantum algorithm for the Simon problem is of the following forms.

First, consider the following quantum algorithm:

(i) Prepare an n-qubit state in the state $|0\rangle$ as the control qubits and an n-qubit state in an arbitrary pure state $|\psi\rangle = \sum_k \alpha_k |k\rangle$ as the auxiliary qubits, (ii) Apply $W_n \otimes I$, (iii) Apply U_f, (iv) Choose a random n-bit string $w = (w_0, \cdots, w_{n-1})$ and apply $S_w = \sigma_z^{w_0} \otimes \cdots \otimes \sigma_z^{w_{n-1}}$ on the n-qubit auxiliary qubits. ($I \otimes S_w$), (v) Apply U_f, (vi) Apply $I \otimes S_w$, (vii) Apply $W_n \otimes I$.

Then the expect probability of obtaining a state $y \in H^+$ is exactly same with that of original Simon algorithm.

In case when the quantum states we are dealing with are mixed state, it is also possible to construct a super operator (more general form of quantum operation) which performs the initialization-free Simon algorithm by means of the unitary operators used above.

Similarly, we can present the initialization-free quantum algorithm for the period-finding problem. Let $f : Z_{2^n} \to Z_{2^n}$ be a periodic function with unknown period *T*.

Instead of Hadamard transformation in initialization-free Simon Algorithm, we use Quantum Fourier Transform F on Z_{2^n} and an m-qubit unitary operation $U_w |y\rangle \to e^{2\pi i wy/m} |-y\rangle$ depending on a random *m*-bit string $w = (w_0, \cdots, w_{n-1})$. That is, (i) Prepare an n-qubit state in the state $|0\rangle$ as the control qubits and an *m*-qubit state in an arbitrary pure state $|\psi\rangle = \sum_k \alpha_k |k\rangle$ as the auxiliary qubits, (ii) Apply $F_n \otimes I$, (iii) Apply U_f, (iv) Apply $I \otimes U_w$, (v) Apply U_f, (vi) Apply $I \otimes U_w$, (vii) Apply $F_n \otimes I$.

Then again, it is quite routine to see that the expect probability of obtaining a state $|y\rangle$ from which, we can get the information of the unknown period is exactly same with that of original period-finding algorithm. The super operator for the case of mixed state can be also constructed by the unitary operators used above.

3.2 Significance to the Field

(1) The limitation on the size of quantum computers makes it important to reuse qubits for auxiliary registers. However, by the algorithmic technique we present here, any arbitrarily mixed state can be used as the auxiliary qubits, and furthermore it can be fully recovered after completing the computations so that the independent processes of several quantum computers can share auxiliary registers. Furthermore, the removal of the preparation in a certain pure state as the initial state of the auxiliary register and full recovery of the original state can make it possible to reuse the recovered one by employing it in any other computations

A single preparation of the auxiliary qubits in an arbitrarily mixed state is sufficient to implement the iterative procedure that is usually necessary in quantum computation and that means an immense reduction of the storage and operations in quantum computing.

(2) It is assumed that most quantum algorithms require some initialization at start-up, which is to prepare a certain pure state as an initial state. However, in experimentally realizable proposals for the implementation of quantum algorithms, it may be technically difficult to prepare and maintain the initial pure state. Especially, the nuclear magnetic resonance (NMR) system is typically applied

to physical systems in equilibrium at room temperature. This means that the initial state of the spins is nearly completely random, that is, it is difficult to prepare pure quantum states of nuclear spins in NMR systems. So our result, by which the initializing steps of a certain pure state can be removed and any initial state can be recovered, would help a lot to avoid such an effort in present-day experimental implementations of quantum computation.

3.3 Relationship to the Original Goals

The original goal was to construct quantum algorithms which can determine certain properties of given mathematical functions in a polynomial time without initializing the input quantum state. That is, quantum algorithms which determines

1. Whether a Boolean function is balanced or not
2. Whether a function is evenly balanced or not
3. Whether a function is evenly distributed or not

in a polynomial times without the initialization of the input state.

As the result of this research, we have accomplished all the contents of our original goals and furthermore, we have constructed a systematic method to construct efficient quantum algorithms solving period-finding problem and Simon's problem without any initialization of the auxiliary register.

It can be also shown that our new method can be applied to various kinds of so called '***hidden subgroup problems***' to which, many problems known to be hard classically have some reductions. Since most of known "exponentially fast" applications of the *Quantum Fourier transform* (QFT) can be considered as a generalization of finding unknown period of a periodic function, the existence of these quantum algorithms implies that any initialization of the auxiliary qubits may be unnecessary in many quantum algorithms.

4. Personnel Supported

None

5. Publication

Dong Pyo Chi, Jeong San Kim and Soojoon Lee, *Quantum algorithms without initializing the auxiliary qubits*, Phys. Rev. Lett. 95, 080504 (2005); Dong Pyo Chi, Jeong San Kim and Soojoon Lee, *Quantum algorithms without initializing the auxiliary qubits* , quant-ph/0504173.

6. Interactions

6.1 Participation at Conferences

(1) KIAS-KAIST 2005 Workshop on Quantum Information Science, Korea Institute for Advanced Study, Seoul, Korea, Aug. 2005.
(2) ERATO Conference on Quantum Information Science, Tokyo, Japan, Aug. 2005.

(3) KMS-KIISC 2005 Joint Workshop ,Chung-Ang University, Seoul, Korea, Oct. 2005.
(4) NATO Advanced Study Institute: Physics and Computer Science, Cargese, Corsica, France, Oct. 2005.
(5) SNU-HU 3rd Joint Symposium on Mathematics, SNU, Seoul, Korea, Oct. 2005.
(6) Conference on Information Security and Cryptology 2005, Seoul National University, Seoul, Korea, Dec. 2005.
(7) The Ninth Workshop on Quantum Information Processing, Paris, France, Jan. 2006.
(8) SNU-Kyoto University Joint Symposium, Kyoto, Japan, Feb. 2006.

6.2 Application Areas

- Symmetric cryptography

Since it is essential to search evenly distributed functions (which are also called regular function) in classical symmetric cryptography to design secure block ciphers, our algorithm can be used in this procedure.

- Complexity class

New quantum algorithms that are exponentially faster than any classical algorithms can be introduced and our work can enlarge some class of quantum computational complexity.

- Present-day experimental implementations of quantum computation

The experimentally realizable proposals for the implementation of quantum algorithms, it may be technically difficult to prepare the initial pure state which has been considered to be necessary. More specifically, in experimental preparation of quantum states by means of the nuclear magnetic resonance (NMR) system, it is known to be difficult to prepare pure quantum states of nuclear spins in NMR systems. Hence, it would be a lot helpful to use our method of quantum algorithms which can be efficiently performed even though the initial states or some parts of them are not in a specific pure state. Furthermore, since the parts of the initial state remain intact even after the computation, the parts could be reused in any other computations, which would save a large amount of the preparation cost in actual physical implementation of quantum algorithms.

7. New Discoveries, Inventions, or patent disclosures

None

8. Honors / Awards

None

9. Archival Documentation

Dong Pyo Chi, Jeong San Kim and Soojoon Lee, *Quantum algorithms without initializing the auxiliary qubits* , Phys. Rev. Lett. 95, 080504 (2005); Dong Pyo Chi, Jeong San Kim and Soojoon Lee, *Quantum algorithms without initializing the auxiliary qubits*, quant-ph/0504173.

10. Software / Hardware

None

11. References

[1] P. W. Shor, FOCS: Proc. 35th IEEE Symp. on the Foundations of Computer Science (Piscataway, NJ: IEEE Computer Society Press) pp. 124-134, 1994; P. W. Shor, SIAM J. Comput. **26** (1997), 1484-1509.
[2] S. Hallgren, in Proceedings of the 34th Annual ACM Symposium on Theory of Computing (Association for Computing Machinery, New York, 2002), pp. 653–658; R. Jozsa, quant-ph/0302134.
[3] D. Deutsch and R. Jozsa, Proc. R. Soc. A 439 (1992) 553-558
[4] D. R. Simon, FOCS: Proc. 35th IEEE Symp. on the Foundations of Computer Science (Piscataway, NJ: IEEE Computer Society Press) pp. 116-123, 1994; D. R. Simon, SIAM J. Comput. 26 (1997), 1474-1483.
[5] G. Brassard, P. Høyer, Proc. of the 5th Israeli Symposium on Theory of Computing Systems, Israel, 1997, pp. 12–23.

PRL 95, 080504 (2005) PHYSICAL REVIEW LETTERS week ending 19 AUGUST 2005

Quantum Algorithms without Initializing the Auxiliary Qubits

Dong Pyo Chi,[1,*] Jeong San Kim,[1,†] and Soojoon Lee[2,‡]

[1]*School of Mathematical Sciences, Seoul National University, Seoul 151-742, Korea*

[2]*Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, Seoul 130-701, Korea*

(Received 27 April 2005; published 17 August 2005)

In this Letter, we construct the quantum algorithms for the Simon problem and the period-finding problem, which do not require initializing the auxiliary qubits involved in the process of functional evaluation but are as efficient as the original algorithms. In these quantum algorithms, one can use any arbitrarily mixed state as the auxiliary qubits, and furthermore can recover the state of the auxiliary qubits to the original one after completing the computations. Since the recovered state can be employed in any other computations, we obtain that a single preparation of the auxiliary qubits in an arbitrarily mixed state is sufficient to implement the iterative procedure in the Simon algorithm or the period-finding algorithm.

DOI: 10.1103/PhysRevLett.95.080504 PACS numbers: 03.67.Lx, 03.65.Ta

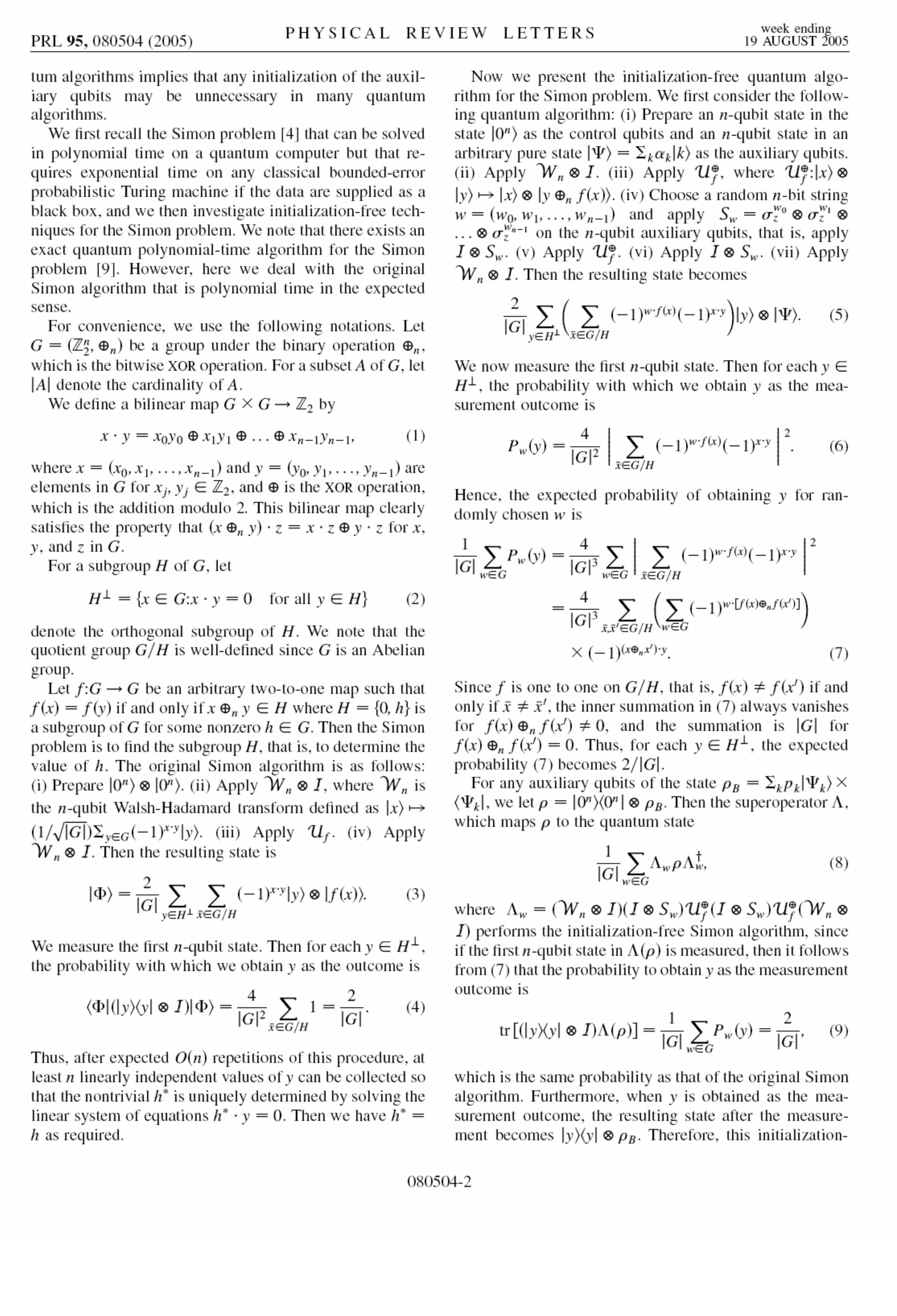
Quantum computational algorithms can be executed in parallel on superpositions of exponentially many input states, and their outcomes can be properly measured by virtue of quantum interference. These enable exponential speedups in the solutions of certain problems and allow one to distinguish between the quantum computational complexity classes and the classical ones [1–10].

It is assumed that most quantum algorithms require some initialization at start-up, which is to prepare a certain pure state as an initial state. However, in experimentally realizable proposals for the implementation of quantum algorithms, it may be technically difficult to prepare the initial pure state. Especially, the nuclear magnetic resonance (NMR) system is typically applied to physical systems in equilibrium at room temperature. This means that the initial state of the spins is nearly completely random, that is, it is difficult to prepare pure quantum states of nuclear spins in NMR systems. Hence, it would be interesting whether quantum algorithms can be efficiently performed even though the initial states or some parts of them are not in a specific pure state. If it would be possible, then the technical difficulty could be settled to a certain extent, and furthermore if the parts of the initial state would remain intact even after the computation, then the parts could be reused in any other computations. We call such a quantum algorithm the *initialization-free quantum algorithm* when any quantum state can be used as the auxiliary (target) qubits involved in the functional evaluation $|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y + f(x)\rangle$ for a given function f, and it can be recovered after the computation.

In the initialization-free quantum algorithms, which are implemented without initializing and deforming the state of the auxiliary qubits, any qubits (which might contain some other useful information) can be temporarily used as the auxiliary qubits, and the initial state of the auxiliary qubits can be recovered at the end of the computation. Thus we can compose the auxiliary qubits of any qubits regardless of whether they are entangled with others or are being used in another computational process. Furthermore, in the case of iterative algorithms, in which one needs to perform the algorithm several times to solve given problems, the initialization-free quantum algorithms can be implemented with the same auxiliary qubits repeatedly, while the original iterative algorithms require the initial auxiliary qubits of a certain pure state at each repetition.

There have been a few research works related to the initialization-free quantum algorithms. Biham *et al.* [11,12] have generalized Grover's algorithm [6] by allowing for an arbitrary initial amplitude distribution, and have shown that Grover's algorithm (or, a large class of Grover-type algorithms) is robust against modest noise in the amplitude initialization procedure. Parker and Plenio [13] found that one pure qubit and an initial supply of $\log_2 N$ qubits in an arbitrarily mixed state are sufficient to implement Shor's quantum factoring algorithm [5] efficiently, where the idea of using one pure qubit and other mixed qubits as the initial state was first introduced by Knill and Laflamme [14]. Their result implies that the controlled unitary transformations in Shor's algorithm can be implemented without any initialization of the auxiliary qubits, while the auxiliary qubits cannot be left in the initial state. Subsequently, Chi *et al.* [15] have presented a quantum algorithm to implement an oracle computing $|x\rangle \mapsto e^{2\pi i f(x)/M}|x\rangle$ for $f:\mathbb{Z}_N \to \mathbb{Z}_M$ by making use of an oracle of the form $|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y + f(x)\rangle$ without setting the auxiliary qubits to a definite state before the computation, and have shown that generalized Deutsch-Jozsa algorithms can be implemented without any initialization of the auxiliary qubits when an oracle computing $\mathcal{U}_f:|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y + f(x)\rangle$ is employed.

In this Letter, we deal with two problems, the Simon problem [4] and the period-finding problem [5], which can be solved efficiently by the quantum computer, and present the initialization-free quantum algorithms for these problems. Since most of known "exponentially fast" applications of the quantum Fourier transform (QFT) can be considered as a generalization of finding an unknown period of a periodic function, the existence of these quan-



tum algorithms implies that any initialization of the auxiliary qubits may be unnecessary in many quantum algorithms.

We first recall the Simon problem [4] that can be solved in polynomial time on a quantum computer but that requires exponential time on any classical bounded-error probabilistic Turing machine if the data are supplied as a black box, and we then investigate initialization-free techniques for the Simon problem. We note that there exists an exact quantum polynomial-time algorithm for the Simon problem [9]. However, here we deal with the original Simon algorithm that is polynomial time in the expected sense.

For convenience, we use the following notations. Let $G = (\mathbb{Z}_2^n, \oplus_n)$ be a group under the binary operation $\oplus_n$, which is the bitwise XOR operation. For a subset A of G, let $|A|$ denote the cardinality of A.

We define a bilinear map $G \times G \to \mathbb{Z}_2$ by

$$x \cdot y = x_0 y_0 \oplus x_1 y_1 \oplus \ldots \oplus x_{n-1} y_{n-1}, \qquad (1)$$

where $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1})$ are elements in G for $x_j, y_j \in \mathbb{Z}_2$, and $\oplus$ is the XOR operation, which is the addition modulo 2. This bilinear map clearly satisfies the property that $(x \oplus_n y) \cdot z = x \cdot z \oplus y \cdot z$ for x, y, and z in G.

For a subgroup H of G, let

$$H^\perp = \{x \in G : x \cdot y = 0 \quad \text{for all } y \in H\} \qquad (2)$$

denote the orthogonal subgroup of H. We note that the quotient group G/H is well-defined since G is an Abelian group.

Let $f: G \to G$ be an arbitrary two-to-one map such that $f(x) = f(y)$ if and only if $x \oplus_n y \in H$ where $H = \{0, h\}$ is a subgroup of G for some nonzero $h \in G$. Then the Simon problem is to find the subgroup H, that is, to determine the value of h. The original Simon algorithm is as follows: (i) Prepare $|0^n\rangle \otimes |0^n\rangle$. (ii) Apply $\mathcal{W}_n \otimes I$, where $\mathcal{W}_n$ is the n-qubit Walsh-Hadamard transform defined as $|x\rangle \mapsto (1/\sqrt{|G|})\Sigma_{y \in G}(-1)^{x \cdot y}|y\rangle$. (iii) Apply $\mathcal{U}_f$. (iv) Apply $\mathcal{W}_n \otimes I$. Then the resulting state is

$$|\Phi\rangle = \frac{2}{|G|} \sum_{y \in H^\perp} \sum_{\bar{x} \in G/H} (-1)^{x \cdot y} |y\rangle \otimes |f(x)\rangle. \qquad (3)$$

We measure the first n-qubit state. Then for each $y \in H^\perp$, the probability with which we obtain y as the outcome is

$$\langle \Phi | (|y\rangle\langle y| \otimes I) | \Phi \rangle = \frac{4}{|G|^2} \sum_{\bar{x} \in G/H} 1 = \frac{2}{|G|}. \qquad (4)$$

Thus, after expected $O(n)$ repetitions of this procedure, at least n linearly independent values of y can be collected so that the nontrivial h^* is uniquely determined by solving the linear system of equations $h^* \cdot y = 0$. Then we have $h^* = h$ as required.

Now we present the initialization-free quantum algorithm for the Simon problem. We first consider the following quantum algorithm: (i) Prepare an n-qubit state in the state $|0^n\rangle$ as the control qubits and an n-qubit state in an arbitrary pure state $|\Psi\rangle = \Sigma_k \alpha_k |k\rangle$ as the auxiliary qubits. (ii) Apply $\mathcal{W}_n \otimes I$. (iii) Apply $\mathcal{U}_f^\oplus$, where $\mathcal{U}_f^\oplus : |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus_n f(x)\rangle$. (iv) Choose a random n-bit string $w = (w_0, w_1, \ldots, w_{n-1})$ and apply $S_w = \sigma_z^{w_0} \otimes \sigma_z^{w_1} \otimes \ldots \otimes \sigma_z^{w_{n-1}}$ on the n-qubit auxiliary qubits, that is, apply $I \otimes S_w$. (v) Apply $\mathcal{U}_f^\oplus$. (vi) Apply $I \otimes S_w$. (vii) Apply $\mathcal{W}_n \otimes I$. Then the resulting state becomes

$$\frac{2}{|G|} \sum_{y \in H^\perp} \left(\sum_{\bar{x} \in G/H} (-1)^{w \cdot f(x)} (-1)^{x \cdot y} \right) |y\rangle \otimes |\Psi\rangle. \qquad (5)$$

We now measure the first n-qubit state. Then for each $y \in H^\perp$, the probability with which we obtain y as the measurement outcome is

$$P_w(y) = \frac{4}{|G|^2} \left| \sum_{\bar{x} \in G/H} (-1)^{w \cdot f(x)} (-1)^{x \cdot y} \right|^2. \qquad (6)$$

Hence, the expected probability of obtaining y for randomly chosen w is

$$\begin{aligned} \frac{1}{|G|} \sum_{w \in G} P_w(y) &= \frac{4}{|G|^3} \sum_{w \in G} \left| \sum_{\bar{x} \in G/H} (-1)^{w \cdot f(x)} (-1)^{x \cdot y} \right|^2 \\ &= \frac{4}{|G|^3} \sum_{\bar{x}, \bar{x}' \in G/H} \left(\sum_{w \in G} (-1)^{w \cdot [f(x) \oplus_n f(x')]} \right) \\ &\quad \times (-1)^{(x \oplus_n x') \cdot y}. \end{aligned} \qquad (7)$$

Since f is one to one on G/H, that is, $f(x) \neq f(x')$ if and only if $\bar{x} \neq \bar{x}'$, the inner summation in (7) always vanishes for $f(x) \oplus_n f(x') \neq 0$, and the summation is $|G|$ for $f(x) \oplus_n f(x') = 0$. Thus, for each $y \in H^\perp$, the expected probability (7) becomes $2/|G|$.

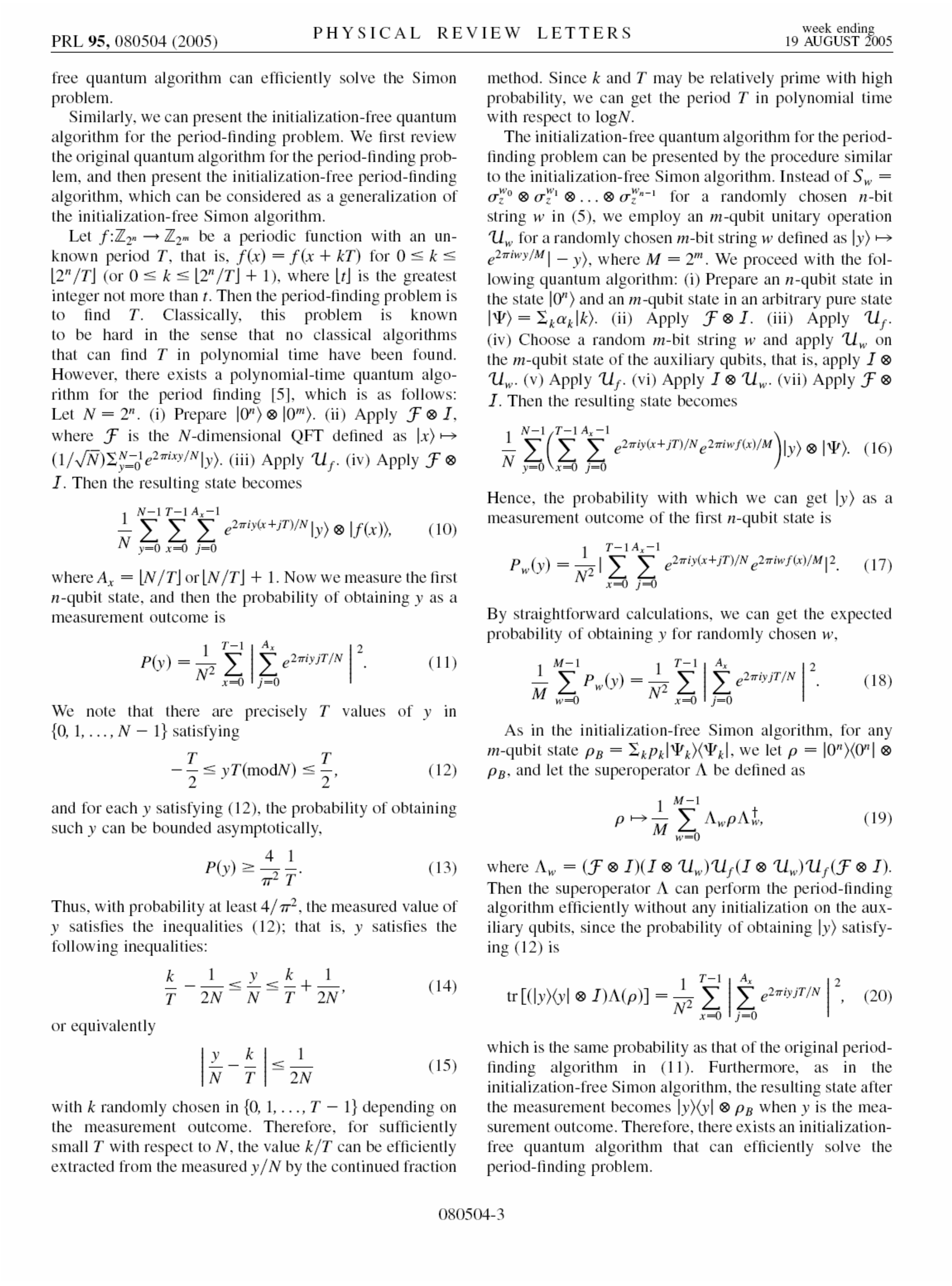
For any auxiliary qubits of the state $\rho_B = \Sigma_k p_k |\Psi_k\rangle \times \langle \Psi_k|$, we let $\rho = |0^n\rangle\langle 0^n| \otimes \rho_B$. Then the superoperator Λ, which maps ρ to the quantum state

$$\frac{1}{|G|} \sum_{w \in G} \Lambda_w \rho \Lambda_w^\dagger, \qquad (8)$$

where $\Lambda_w = (\mathcal{W}_n \otimes I)(I \otimes S_w)\mathcal{U}_f^\oplus(I \otimes S_w)\mathcal{U}_f^\oplus(\mathcal{W}_n \otimes I)$ performs the initialization-free Simon algorithm, since if the first n-qubit state in $\Lambda(\rho)$ is measured, then it follows from (7) that the probability to obtain y as the measurement outcome is

$$\mathrm{tr}\,[(|y\rangle\langle y| \otimes I)\Lambda(\rho)] = \frac{1}{|G|} \sum_{w \in G} P_w(y) = \frac{2}{|G|}, \qquad (9)$$

which is the same probability as that of the original Simon algorithm. Furthermore, when y is obtained as the measurement outcome, the resulting state after the measurement becomes $|y\rangle\langle y| \otimes \rho_B$. Therefore, this initialization-



free quantum algorithm can efficiently solve the Simon problem.

Similarly, we can present the initialization-free quantum algorithm for the period-finding problem. We first review the original quantum algorithm for the period-finding problem, and then present the initialization-free period-finding algorithm, which can be considered as a generalization of the initialization-free Simon algorithm.

Let $f:\mathbb{Z}_{2^n} \to \mathbb{Z}_{2^m}$ be a periodic function with an unknown period T, that is, $f(x) = f(x + kT)$ for $0 \le k \le \lfloor 2^n/T \rfloor$ (or $0 \le k \le \lfloor 2^n/T \rfloor + 1$), where $\lfloor t \rfloor$ is the greatest integer not more than t. Then the period-finding problem is to find T. Classically, this problem is known to be hard in the sense that no classical algorithms that can find T in polynomial time have been found. However, there exists a polynomial-time quantum algorithm for the period finding [5], which is as follows: Let $N = 2^n$. (i) Prepare $|0^n\rangle \otimes |0^m\rangle$. (ii) Apply $\mathcal{F} \otimes \mathcal{I}$, where $\mathcal{F}$ is the N-dimensional QFT defined as $|x\rangle \mapsto (1/\sqrt{N})\Sigma_{y=0}^{N-1} e^{2\pi ixy/N}|y\rangle$. (iii) Apply $\mathcal{U}_f$. (iv) Apply $\mathcal{F} \otimes \mathcal{I}$. Then the resulting state becomes

$$\frac{1}{N}\sum_{y=0}^{N-1}\sum_{x=0}^{T-1}\sum_{j=0}^{A_x-1} e^{2\pi iy(x+jT)/N}|y\rangle \otimes |f(x)\rangle, \qquad (10)$$

where $A_x = \lfloor N/T \rfloor$ or $\lfloor N/T \rfloor + 1$. Now we measure the first n-qubit state, and then the probability of obtaining y as a measurement outcome is

$$P(y) = \frac{1}{N^2}\sum_{x=0}^{T-1}\left|\sum_{j=0}^{A_x} e^{2\pi iyjT/N}\right|^2. \qquad (11)$$

We note that there are precisely T values of y in $\{0, 1, \ldots, N-1\}$ satisfying

$$-\frac{T}{2} \le yT(\mathrm{mod}N) \le \frac{T}{2}, \qquad (12)$$

and for each y satisfying (12), the probability of obtaining such y can be bounded asymptotically,

$$P(y) \ge \frac{4}{\pi^2}\frac{1}{T}. \qquad (13)$$

Thus, with probability at least $4/\pi^2$, the measured value of y satisfies the inequalities (12); that is, y satisfies the following inequalities:

$$\frac{k}{T} - \frac{1}{2N} \le \frac{y}{N} \le \frac{k}{T} + \frac{1}{2N}, \qquad (14)$$

or equivalently

$$\left|\frac{y}{N} - \frac{k}{T}\right| \le \frac{1}{2N} \qquad (15)$$

with k randomly chosen in $\{0, 1, \ldots, T-1\}$ depending on the measurement outcome. Therefore, for sufficiently small T with respect to N, the value k/T can be efficiently extracted from the measured y/N by the continued fraction method. Since k and T may be relatively prime with high probability, we can get the period T in polynomial time with respect to log$N$.

The initialization-free quantum algorithm for the period-finding problem can be presented by the procedure similar to the initialization-free Simon algorithm. Instead of $S_w = \sigma_z^{w_0} \otimes \sigma_z^{w_1} \otimes \ldots \otimes \sigma_z^{w_{n-1}}$ for a randomly chosen n-bit string w in (5), we employ an m-qubit unitary operation $\mathcal{U}_w$ for a randomly chosen m-bit string w defined as $|y\rangle \mapsto e^{2\pi iwy/M}|-y\rangle$, where $M = 2^m$. We proceed with the following quantum algorithm: (i) Prepare an n-qubit state in the state $|0^n\rangle$ and an m-qubit state in an arbitrary pure state $|\Psi\rangle = \Sigma_k\alpha_k|k\rangle$. (ii) Apply $\mathcal{F} \otimes \mathcal{I}$. (iii) Apply $\mathcal{U}_f$. (iv) Choose a random m-bit string w and apply $\mathcal{U}_w$ on the m-qubit state of the auxiliary qubits, that is, apply $\mathcal{I} \otimes \mathcal{U}_w$. (v) Apply $\mathcal{U}_f$. (vi) Apply $\mathcal{I} \otimes \mathcal{U}_w$. (vii) Apply $\mathcal{F} \otimes \mathcal{I}$. Then the resulting state becomes

$$\frac{1}{N}\sum_{y=0}^{N-1}\left(\sum_{x=0}^{T-1}\sum_{j=0}^{A_x-1} e^{2\pi iy(x+jT)/N}e^{2\pi iwf(x)/M}\right)|y\rangle \otimes |\Psi\rangle. \qquad (16)$$

Hence, the probability with which we can get $|y\rangle$ as a measurement outcome of the first n-qubit state is

$$P_w(y) = \frac{1}{N^2}|\sum_{x=0}^{T-1}\sum_{j=0}^{A_x-1} e^{2\pi iy(x+jT)/N}e^{2\pi iwf(x)/M}|^2. \qquad (17)$$

By straightforward calculations, we can get the expected probability of obtaining y for randomly chosen w,

$$\frac{1}{M}\sum_{w=0}^{M-1}P_w(y) = \frac{1}{N^2}\sum_{x=0}^{T-1}\left|\sum_{j=0}^{A_x} e^{2\pi iyjT/N}\right|^2. \qquad (18)$$

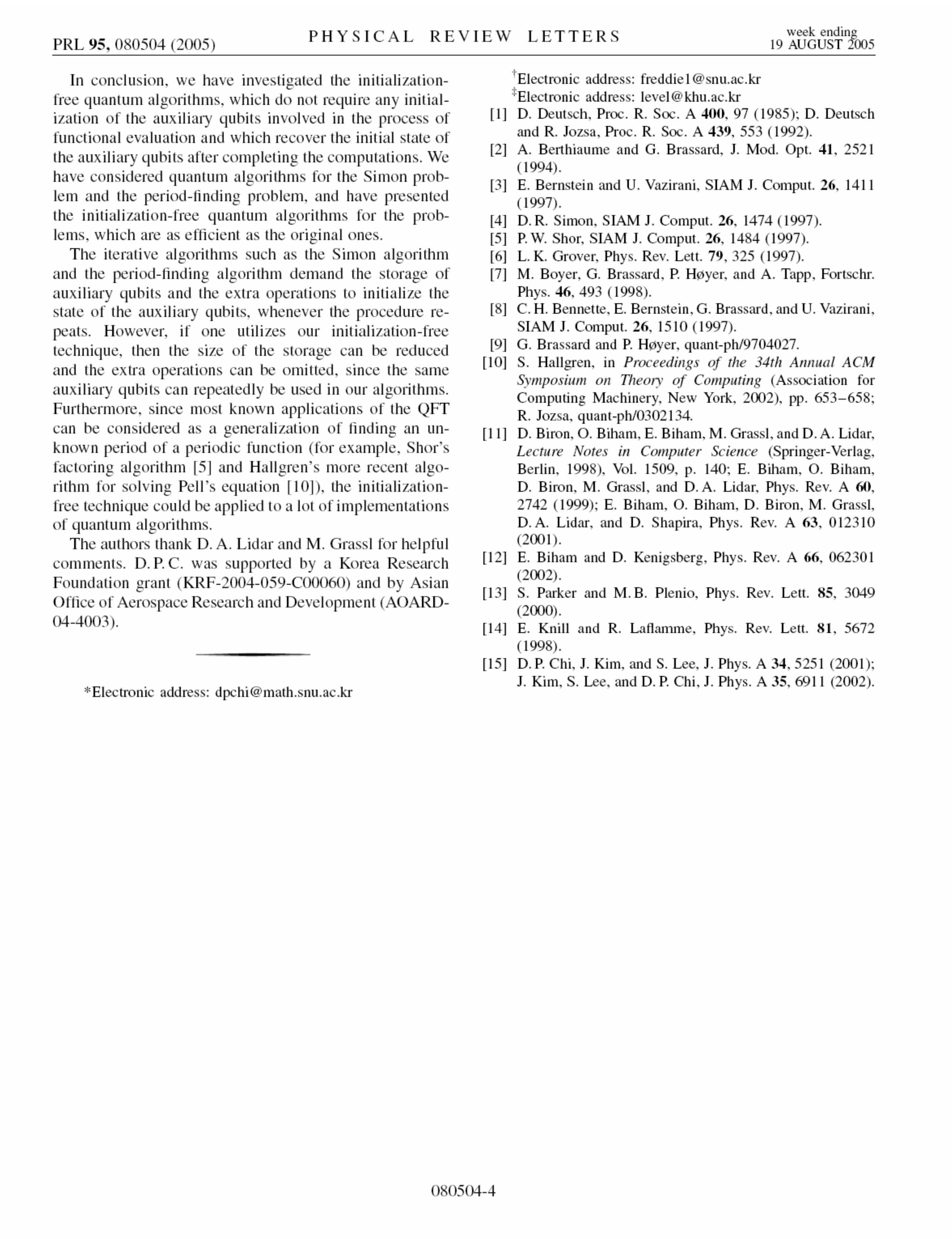
As in the initialization-free Simon algorithm, for any m-qubit state $\rho_B = \Sigma_k p_k|\Psi_k\rangle\langle\Psi_k|$, we let $\rho = |0^n\rangle\langle 0^n| \otimes \rho_B$, and let the superoperator Λ be defined as

$$\rho \mapsto \frac{1}{M}\sum_{w=0}^{M-1}\Lambda_w\rho\Lambda_w^\dagger, \qquad (19)$$

where $\Lambda_w = (\mathcal{F} \otimes \mathcal{I})(\mathcal{I} \otimes \mathcal{U}_w)\mathcal{U}_f(\mathcal{I} \otimes \mathcal{U}_w)\mathcal{U}_f(\mathcal{F} \otimes \mathcal{I})$. Then the superoperator Λ can perform the period-finding algorithm efficiently without any initialization on the auxiliary qubits, since the probability of obtaining $|y\rangle$ satisfying (12) is

$$\mathrm{tr}[(|y\rangle\langle y| \otimes \mathcal{I})\Lambda(\rho)] = \frac{1}{N^2}\sum_{x=0}^{T-1}\left|\sum_{j=0}^{A_x} e^{2\pi iyjT/N}\right|^2, \qquad (20)$$

which is the same probability as that of the original period-finding algorithm in (11). Furthermore, as in the initialization-free Simon algorithm, the resulting state after the measurement becomes $|y\rangle\langle y| \otimes \rho_B$ when y is the measurement outcome. Therefore, there exists an initialization-free quantum algorithm that can efficiently solve the period-finding problem.



In conclusion, we have investigated the initialization-free quantum algorithms, which do not require any initialization of the auxiliary qubits involved in the process of functional evaluation and which recover the initial state of the auxiliary qubits after completing the computations. We have considered quantum algorithms for the Simon problem and the period-finding problem, and have presented the initialization-free quantum algorithms for the problems, which are as efficient as the original ones.

The iterative algorithms such as the Simon algorithm and the period-finding algorithm demand the storage of auxiliary qubits and the extra operations to initialize the state of the auxiliary qubits, whenever the procedure repeats. However, if one utilizes our initialization-free technique, then the size of the storage can be reduced and the extra operations can be omitted, since the same auxiliary qubits can repeatedly be used in our algorithms. Furthermore, since most known applications of the QFT can be considered as a generalization of finding an unknown period of a periodic function (for example, Shor's factoring algorithm [5] and Hallgren's more recent algorithm for solving Pell's equation [10]), the initialization-free technique could be applied to a lot of implementations of quantum algorithms.

The authors thank D. A. Lidar and M. Grassl for helpful comments. D. P. C. was supported by a Korea Research Foundation grant (KRF-2004-059-C00060) and by Asian Office of Aerospace Research and Development (AOARD-04-4003).

*Electronic address: dpchi@math.snu.ac.kr

†Electronic address: freddie1@snu.ac.kr

‡Electronic address: level@khu.ac.kr

[1] D. Deutsch, Proc. R. Soc. A **400**, 97 (1985); D. Deutsch and R. Jozsa, Proc. R. Soc. A **439**, 553 (1992).

[2] A. Berthiaume and G. Brassard, J. Mod. Opt. **41**, 2521 (1994).

[3] E. Bernstein and U. Vazirani, SIAM J. Comput. **26**, 1411 (1997).

[4] D. R. Simon, SIAM J. Comput. **26**, 1474 (1997).

[5] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).

[6] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[7] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, Fortschr. Phys. **46**, 493 (1998).

[8] C. H. Bennette, E. Bernstein, G. Brassard, and U. Vazirani, SIAM J. Comput. **26**, 1510 (1997).

[9] G. Brassard and P. Høyer, quant-ph/9704027.

[10] S. Hallgren, in *Proceedings of the 34th Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, New York, 2002), pp. 653–658; R. Jozsa, quant-ph/0302134.

[11] D. Biron, O. Biham, E. Biham, M. Grassl, and D. A. Lidar, *Lecture Notes in Computer Science* (Springer-Verlag, Berlin, 1998), Vol. 1509, p. 140; E. Biham, O. Biham, D. Biron, M. Grassl, and D. A. Lidar, Phys. Rev. A **60**, 2742 (1999); E. Biham, O. Biham, D. Biron, M. Grassl, D. A. Lidar, and D. Shapira, Phys. Rev. A **63**, 012310 (2001).

[12] E. Biham and D. Kenigsberg, Phys. Rev. A **66**, 062301 (2002).

[13] S. Parker and M. B. Plenio, Phys. Rev. Lett. **85**, 3049 (2000).

[14] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).

[15] D. P. Chi, J. Kim, and S. Lee, J. Phys. A **34**, 5251 (2001); J. Kim, S. Lee, and D. P. Chi, J. Phys. A **35**, 6911 (2002).

Quantum algorithms without initializing the auxiliary qubits

Dong Pyo Chi,[1,*] Jeong San Kim,[1,†] and Soojoon Lee[2,‡]

[1] *School of Mathematical Sciences, Seoul National University, Seoul 151-742, Korea*

[2] *Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, Seoul 130-701, Korea*

(Dated: August 30, 2006)

In this Letter, we construct the quantum algorithms for the Simon problem and the period-finding problem, which do not require initializing the auxiliary qubits involved in the process of functional evaluation but are as efficient as the original algorithms. In these quantum algorithms, one can use any arbitrarily mixed state as the auxiliary qubits, and furthermore can recover the state of the auxiliary qubits to the original one after completing the computations. Since the recovered state can be employed in any other computations, we obtain that a single preparation of the auxiliary qubits in an arbitrarily mixed state is sufficient to implement the iterative procedure in the Simon algorithm or the period-finding algorithm.

PACS numbers: 03.67.Lx, 03.65.Ta

Quantum computational algorithms can be executed in parallel on superpositions of exponentially many input states, and their outcomes can be properly measured by virtue of quantum interference. These enable exponential speedups in the solutions of certain problems, and allow one to distinguish between the quantum computational complexity classes and the classical ones [1, 2, 3, 4, 5, 6, 7, 8, 9, 10].

It is assumed that most quantum algorithms require some initialization at start-up, which is to prepare a certain pure state as an initial state. However, in experimentally realizable proposals for the implementation of quantum algorithms, it may be technically difficult to prepare the initial pure state. Especially, the nuclear magnetic resonance (NMR) system is typically applied to physical systems in equilibrium at room temperature. This means that the initial state of the spins is nearly completely random, that is, it is difficult to prepare pure quantum states of nuclear spins in NMR systems. Hence, it would be interesting whether quantum algorithms can be efficiently performed even though the initial states or some parts of them are not in a specific pure state. If it would be possible, then the technical difficulty could be settled to a certain extent, and furthermore if the parts of the initial state would remain intact even after the computation, then the parts could be reused in any other computations. We call such a quantum algorithm the *initialization-free quantum algorithm* when any quantum state can be used as the auxiliary (target) qubits involved in the functional evaluation $|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y + f(x)\rangle$ for a given function f, and it can be recovered after the computation.

In the initialization-free quantum algorithms, which are implemented without initializing and deforming the state of the auxiliary qubits, any qubits (which might contain some other useful information) can be temporarily used as the auxiliary qubits, and the initial state of the auxiliary qubits can be recovered at the end of the computation. Thus we can compose the auxiliary qubits of any qubits regardless of whether they are entangled with others or being used in another computational process. Furthermore, in the case of iterative algorithms, in which one needs to perform the algorithm several times to solve given problems, the initialization-free quantum algorithms can be implemented with the same auxiliary qubits repeatedly, while the original iterative algorithms require the initial auxiliary qubits of a certain pure state at each repetition.

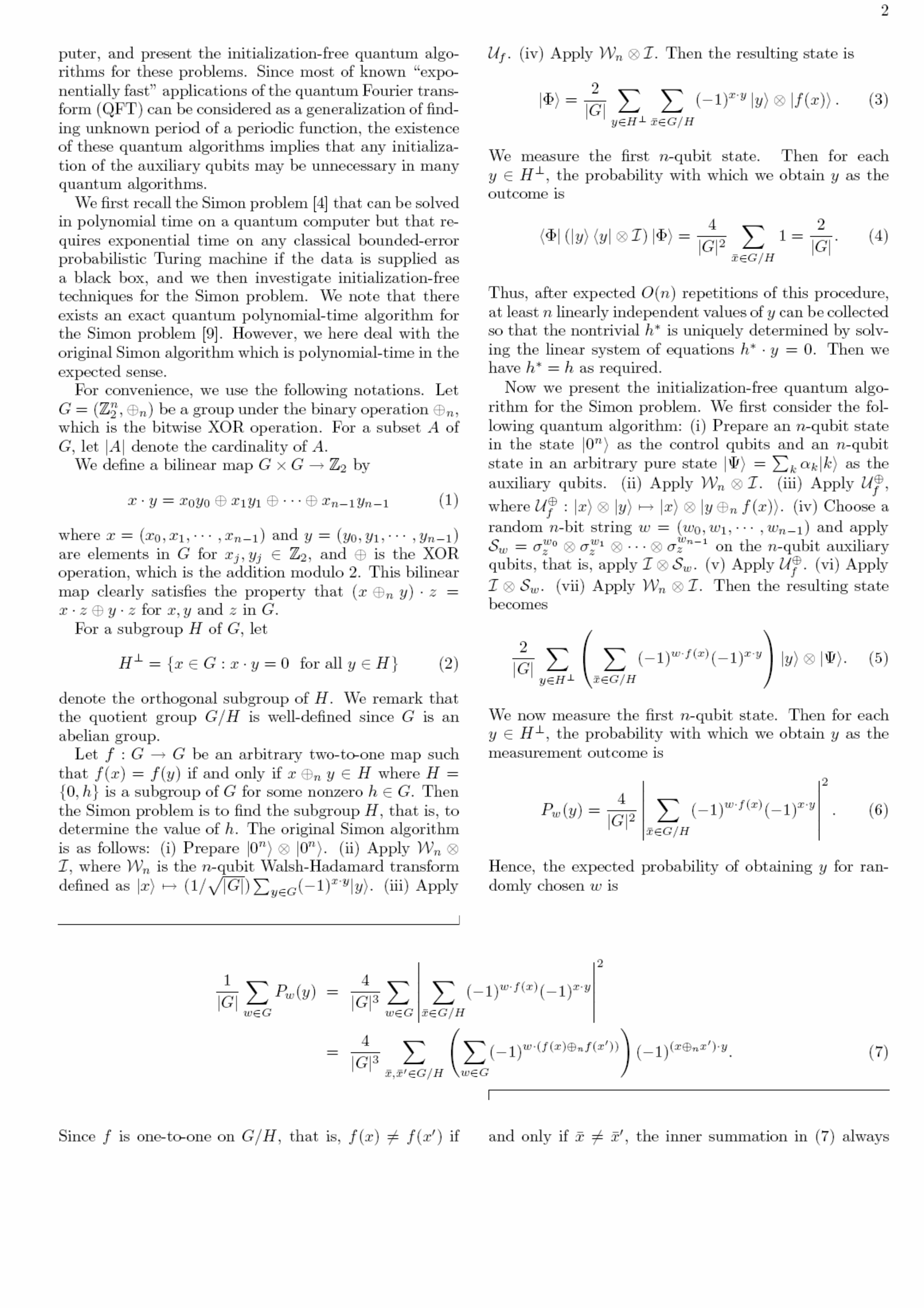
There have been a few research works related to the initialization-free quantum algorithms. Biham *et al.* [11, 12] have generalized Grover's algorithm [6] by allowing for an arbitrary initial amplitude distribution, and have shown that Grover's algorithm (or, a large class of Grover-type algorithms) is robust against modest noise in the amplitude initialization procedure. Parker and Plenio [13] found that one pure qubit and an initial supply of $\log_2 N$ qubits in an arbitrarily mixed state are sufficient to implement Shor's quantum factoring algorithm [5] efficiently, where the idea of using one pure qubit and other mixed qubits as the initial state was first introduced by Knill and Laflamme [14]. Their result implies that the controlled unitary transformations in Shor's algorithm can be implemented without any initialization of the auxiliary qubits, while the auxiliary qubits cannot be left in the initial state. Subsequently, Chi *et al.* [15] have presented a quantum algorithm to implement an oracle computing $|x\rangle \mapsto e^{2\pi i f(x)/M}|x\rangle$ for $f : \mathbb{Z}_N \to \mathbb{Z}_M$ by making use of an oracle of the form $|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y + f(x)\rangle$ without setting the auxiliary qubits to a definite state before the computation, and have shown that generalized Deutsch-Jozsa algorithms can be implemented without any initialization of the auxiliary qubits when an oracle computing $\mathcal{U}_f : |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y + f(x)\rangle$ is employed.

In this Letter, we deal with two problems, the Simon problem [4] and the period-finding problem [5], which can be solved efficiently by the quantum com-

[*] Electronic address: dpchi@math.snu.ac.kr

[†] Electronic address: freddie1@snu.ac.kr

[‡] Electronic address: level@khu.ac.kr



puter, and present the initialization-free quantum algorithms for these problems. Since most of known "exponentially fast" applications of the quantum Fourier transform (QFT) can be considered as a generalization of finding unknown period of a periodic function, the existence of these quantum algorithms implies that any initialization of the auxiliary qubits may be unnecessary in many quantum algorithms.

We first recall the Simon problem [4] that can be solved in polynomial time on a quantum computer but that requires exponential time on any classical bounded-error probabilistic Turing machine if the data is supplied as a black box, and we then investigate initialization-free techniques for the Simon problem. We note that there exists an exact quantum polynomial-time algorithm for the Simon problem [9]. However, we here deal with the original Simon algorithm which is polynomial-time in the expected sense.

For convenience, we use the following notations. Let $G = (\mathbb{Z}_2^n, \oplus_n)$ be a group under the binary operation $\oplus_n$, which is the bitwise XOR operation. For a subset A of G, let $|A|$ denote the cardinality of A.

We define a bilinear map $G \times G \to \mathbb{Z}_2$ by

$$x \cdot y = x_0 y_0 \oplus x_1 y_1 \oplus \cdots \oplus x_{n-1} y_{n-1} \tag{1}$$

where $x = (x_0, x_1, \cdots, x_{n-1})$ and $y = (y_0, y_1, \cdots, y_{n-1})$ are elements in G for $x_j, y_j \in \mathbb{Z}_2$, and $\oplus$ is the XOR operation, which is the addition modulo 2. This bilinear map clearly satisfies the property that $(x \oplus_n y) \cdot z = x \cdot z \oplus y \cdot z$ for x, y and z in G.

For a subgroup H of G, let

$$H^\perp = \{x \in G : x \cdot y = 0 \quad \text{for all } y \in H\} \tag{2}$$

denote the orthogonal subgroup of H. We remark that the quotient group G/H is well-defined since G is an abelian group.

Let $f : G \to G$ be an arbitrary two-to-one map such that $f(x) = f(y)$ if and only if $x \oplus_n y \in H$ where $H = \{0, h\}$ is a subgroup of G for some nonzero $h \in G$. Then the Simon problem is to find the subgroup H, that is, to determine the value of h. The original Simon algorithm is as follows: (i) Prepare $|0^n\rangle \otimes |0^n\rangle$. (ii) Apply $\mathcal{W}_n \otimes \mathcal{I}$, where $\mathcal{W}_n$ is the n-qubit Walsh-Hadamard transform defined as $|x\rangle \mapsto (1/\sqrt{|G|}) \sum_{y \in G} (-1)^{x \cdot y} |y\rangle$. (iii) Apply $\mathcal{U}_f$. (iv) Apply $\mathcal{W}_n \otimes \mathcal{I}$. Then the resulting state is

$$|\Phi\rangle = \frac{2}{|G|} \sum_{y \in H^\perp} \sum_{\bar{x} \in G/H} (-1)^{x \cdot y} |y\rangle \otimes |f(x)\rangle . \tag{3}$$

We measure the first n-qubit state. Then for each $y \in H^\perp$, the probability with which we obtain y as the outcome is

$$\langle \Phi | (|y\rangle \langle y| \otimes \mathcal{I}) |\Phi\rangle = \frac{4}{|G|^2} \sum_{\bar{x} \in G/H} 1 = \frac{2}{|G|}. \tag{4}$$

Thus, after expected $O(n)$ repetitions of this procedure, at least n linearly independent values of y can be collected so that the nontrivial h^* is uniquely determined by solving the linear system of equations $h^* \cdot y = 0$. Then we have $h^* = h$ as required.

Now we present the initialization-free quantum algorithm for the Simon problem. We first consider the following quantum algorithm: (i) Prepare an n-qubit state in the state $|0^n\rangle$ as the control qubits and an n-qubit state in an arbitrary pure state $|\Psi\rangle = \sum_k \alpha_k |k\rangle$ as the auxiliary qubits. (ii) Apply $\mathcal{W}_n \otimes \mathcal{I}$. (iii) Apply $\mathcal{U}_f^\oplus$, where $\mathcal{U}_f^\oplus : |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus_n f(x)\rangle$. (iv) Choose a random n-bit string $w = (w_0, w_1, \cdots, w_{n-1})$ and apply $\mathcal{S}_w = \sigma_z^{w_0} \otimes \sigma_z^{w_1} \otimes \cdots \otimes \sigma_z^{w_{n-1}}$ on the n-qubit auxiliary qubits, that is, apply $\mathcal{I} \otimes \mathcal{S}_w$. (v) Apply $\mathcal{U}_f^\oplus$. (vi) Apply $\mathcal{I} \otimes \mathcal{S}_w$. (vii) Apply $\mathcal{W}_n \otimes \mathcal{I}$. Then the resulting state becomes

$$\frac{2}{|G|} \sum_{y \in H^\perp} \left(\sum_{\bar{x} \in G/H} (-1)^{w \cdot f(x)} (-1)^{x \cdot y} \right) |y\rangle \otimes |\Psi\rangle. \tag{5}$$

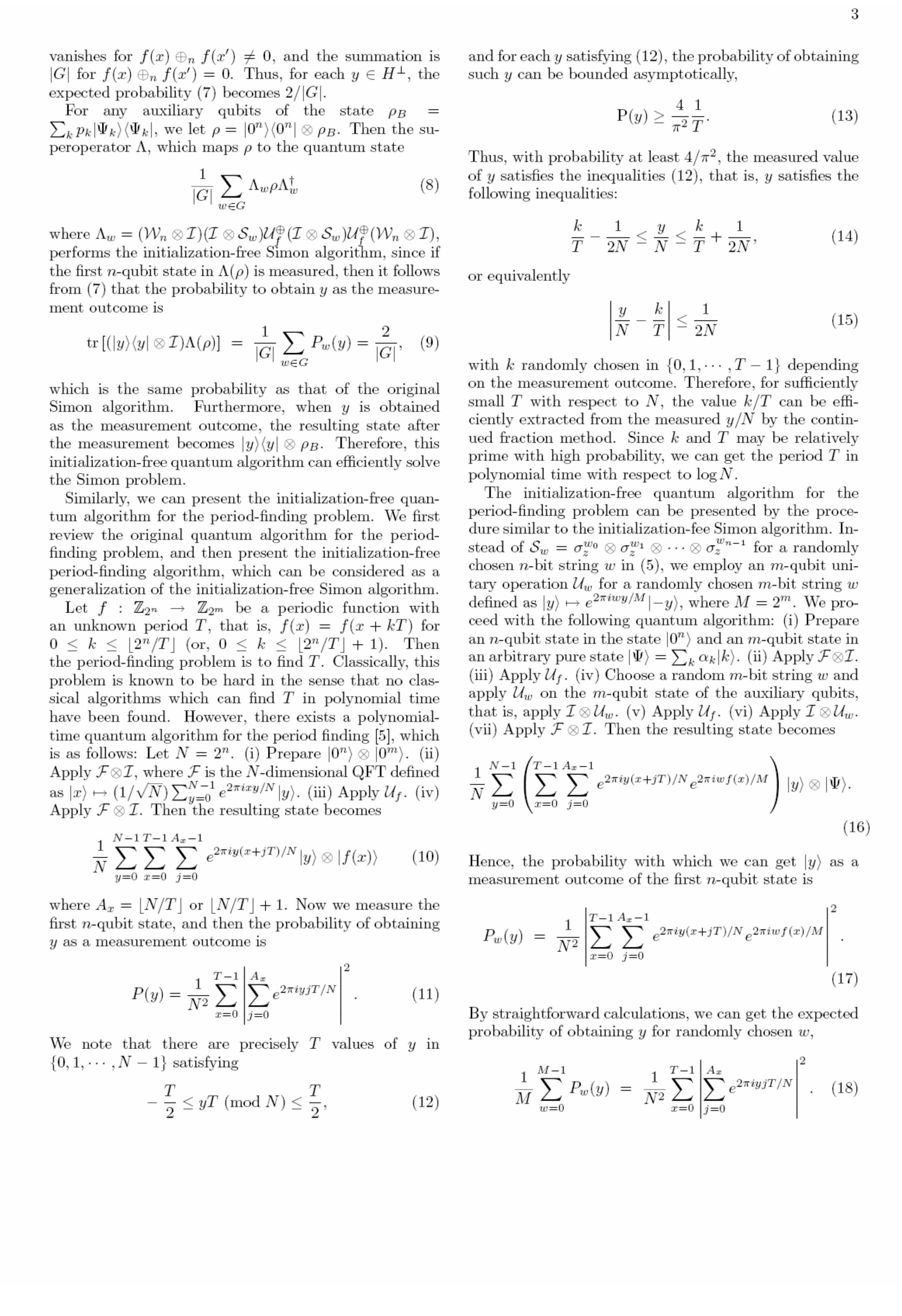
We now measure the first n-qubit state. Then for each $y \in H^\perp$, the probability with which we obtain y as the measurement outcome is

$$P_w(y) = \frac{4}{|G|^2} \left| \sum_{\bar{x} \in G/H} (-1)^{w \cdot f(x)} (-1)^{x \cdot y} \right|^2 . \tag{6}$$

Hence, the expected probability of obtaining y for randomly chosen w is

$$\begin{aligned} \frac{1}{|G|} \sum_{w \in G} P_w(y) &= \frac{4}{|G|^3} \sum_{w \in G} \left| \sum_{\bar{x} \in G/H} (-1)^{w \cdot f(x)} (-1)^{x \cdot y} \right|^2 \\ &= \frac{4}{|G|^3} \sum_{\bar{x}, \bar{x}' \in G/H} \left(\sum_{w \in G} (-1)^{w \cdot (f(x) \oplus_n f(x'))} \right) (-1)^{(x \oplus_n x') \cdot y}. \end{aligned} \tag{7}$$

Since f is one-to-one on G/H, that is, $f(x) \neq f(x')$ if and only if $\bar{x} \neq \bar{x}'$, the inner summation in (7) always



vanishes for $f(x) \oplus_n f(x') \neq 0$, and the summation is $|G|$ for $f(x) \oplus_n f(x') = 0$. Thus, for each $y \in H^\perp$, the expected probability (7) becomes $2/|G|$.

For any auxiliary qubits of the state $\rho_B = \sum_k p_k |\Psi_k\rangle\langle\Psi_k|$, we let $\rho = |0^n\rangle\langle 0^n| \otimes \rho_B$. Then the superoperator Λ, which maps ρ to the quantum state

$$\frac{1}{|G|} \sum_{w \in G} \Lambda_w \rho \Lambda_w^\dagger \tag{8}$$

where $\Lambda_w = (\mathcal{W}_n \otimes \mathcal{I})(\mathcal{I} \otimes \mathcal{S}_w)\mathcal{U}_f^\oplus(\mathcal{I} \otimes \mathcal{S}_w)\mathcal{U}_f^\oplus(\mathcal{W}_n \otimes \mathcal{I})$, performs the initialization-free Simon algorithm, since if the first n-qubit state in $\Lambda(\rho)$ is measured, then it follows from (7) that the probability to obtain y as the measurement outcome is

$$\mathrm{tr}\left[(|y\rangle\langle y| \otimes \mathcal{I})\Lambda(\rho)\right] \;=\; \frac{1}{|G|} \sum_{w \in G} P_w(y) = \frac{2}{|G|}, \tag{9}$$

which is the same probability as that of the original Simon algorithm. Furthermore, when y is obtained as the measurement outcome, the resulting state after the measurement becomes $|y\rangle\langle y| \otimes \rho_B$. Therefore, this initialization-free quantum algorithm can efficiently solve the Simon problem.

Similarly, we can present the initialization-free quantum algorithm for the period-finding problem. We first review the original quantum algorithm for the period-finding problem, and then present the initialization-free period-finding algorithm, which can be considered as a generalization of the initialization-free Simon algorithm.

Let $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^m}$ be a periodic function with an unknown period T, that is, $f(x) = f(x + kT)$ for $0 \leq k \leq \lfloor 2^n/T \rfloor$ (or, $0 \leq k \leq \lfloor 2^n/T \rfloor + 1$). Then the period-finding problem is to find T. Classically, this problem is known to be hard in the sense that no classical algorithms which can find T in polynomial time have been found. However, there exists a polynomial-time quantum algorithm for the period finding [5], which is as follows: Let $N = 2^n$. (i) Prepare $|0^n\rangle \otimes |0^m\rangle$. (ii) Apply $\mathcal{F} \otimes \mathcal{I}$, where $\mathcal{F}$ is the N-dimensional QFT defined as $|x\rangle \mapsto (1/\sqrt{N}) \sum_{y=0}^{N-1} e^{2\pi i x y/N} |y\rangle$. (iii) Apply $\mathcal{U}_f$. (iv) Apply $\mathcal{F} \otimes \mathcal{I}$. Then the resulting state becomes

$$\frac{1}{N} \sum_{y=0}^{N-1} \sum_{x=0}^{T-1} \sum_{j=0}^{A_x - 1} e^{2\pi i y(x+jT)/N} |y\rangle \otimes |f(x)\rangle \tag{10}$$

where $A_x = \lfloor N/T \rfloor$ or $\lfloor N/T \rfloor + 1$. Now we measure the first n-qubit state, and then the probability of obtaining y as a measurement outcome is

$$P(y) = \frac{1}{N^2} \sum_{x=0}^{T-1} \left| \sum_{j=0}^{A_x} e^{2\pi i y j T/N} \right|^2. \tag{11}$$

We note that there are precisely T values of y in $\{0, 1, \cdots, N-1\}$ satisfying

$$-\frac{T}{2} \leq yT \ (\mathrm{mod}\ N) \leq \frac{T}{2}, \tag{12}$$

and for each y satisfying (12), the probability of obtaining such y can be bounded asymptotically,

$$\mathrm{P}(y) \geq \frac{4}{\pi^2} \frac{1}{T}. \tag{13}$$

Thus, with probability at least $4/\pi^2$, the measured value of y satisfies the inequalities (12), that is, y satisfies the following inequalities:

$$\frac{k}{T} - \frac{1}{2N} \leq \frac{y}{N} \leq \frac{k}{T} + \frac{1}{2N}, \tag{14}$$

or equivalently

$$\left| \frac{y}{N} - \frac{k}{T} \right| \leq \frac{1}{2N} \tag{15}$$

with k randomly chosen in $\{0, 1, \cdots, T-1\}$ depending on the measurement outcome. Therefore, for sufficiently small T with respect to N, the value k/T can be efficiently extracted from the measured y/N by the continued fraction method. Since k and T may be relatively prime with high probability, we can get the period T in polynomial time with respect to $\log N$.

The initialization-free quantum algorithm for the period-finding problem can be presented by the procedure similar to the initialization-fee Simon algorithm. Instead of $\mathcal{S}_w = \sigma_z^{w_0} \otimes \sigma_z^{w_1} \otimes \cdots \otimes \sigma_z^{w_{n-1}}$ for a randomly chosen n-bit string w in (5), we employ an m-qubit unitary operation $\mathcal{U}_w$ for a randomly chosen m-bit string w defined as $|y\rangle \mapsto e^{2\pi i w y/M} |-y\rangle$, where $M = 2^m$. We proceed with the following quantum algorithm: (i) Prepare an n-qubit state in the state $|0^n\rangle$ and an m-qubit state in an arbitrary pure state $|\Psi\rangle = \sum_k \alpha_k |k\rangle$. (ii) Apply $\mathcal{F} \otimes \mathcal{I}$. (iii) Apply $\mathcal{U}_f$. (iv) Choose a random m-bit string w and apply $\mathcal{U}_w$ on the m-qubit state of the auxiliary qubits, that is, apply $\mathcal{I} \otimes \mathcal{U}_w$. (v) Apply $\mathcal{U}_f$. (vi) Apply $\mathcal{I} \otimes \mathcal{U}_w$. (vii) Apply $\mathcal{F} \otimes \mathcal{I}$. Then the resulting state becomes

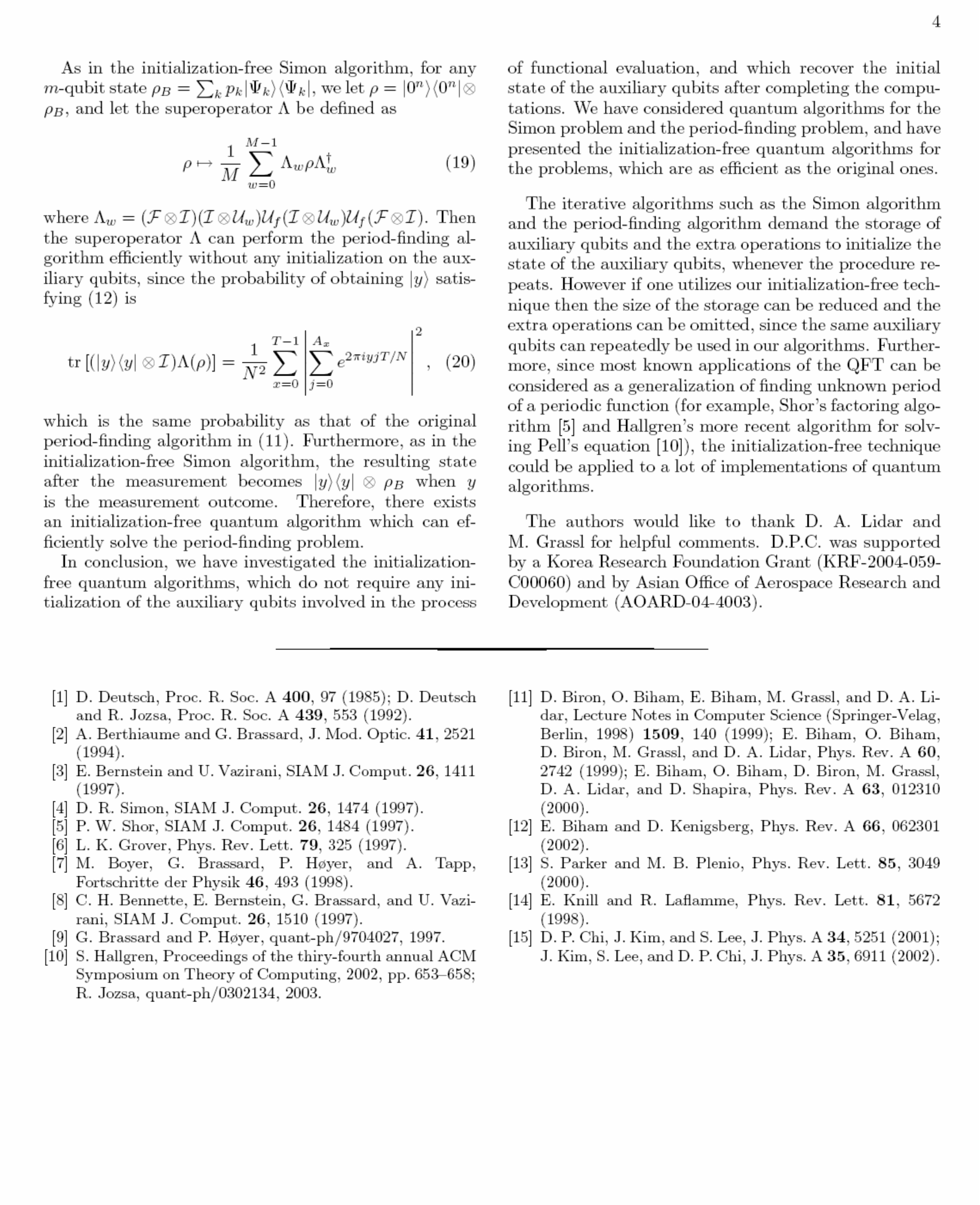
$$\frac{1}{N} \sum_{y=0}^{N-1} \left(\sum_{x=0}^{T-1} \sum_{j=0}^{A_x - 1} e^{2\pi i y(x+jT)/N} e^{2\pi i w f(x)/M} \right) |y\rangle \otimes |\Psi\rangle. \tag{16}$$

Hence, the probability with which we can get $|y\rangle$ as a measurement outcome of the first n-qubit state is

$$P_w(y) \;=\; \frac{1}{N^2} \left| \sum_{x=0}^{T-1} \sum_{j=0}^{A_x - 1} e^{2\pi i y(x+jT)/N} e^{2\pi i w f(x)/M} \right|^2. \tag{17}$$

By straightforward calculations, we can get the expected probability of obtaining y for randomly chosen w,

$$\frac{1}{M} \sum_{w=0}^{M-1} P_w(y) \;=\; \frac{1}{N^2} \sum_{x=0}^{T-1} \left| \sum_{j=0}^{A_x} e^{2\pi i y j T/N} \right|^2. \tag{18}$$



As in the initialization-free Simon algorithm, for any m-qubit state $\rho_B = \sum_k p_k |\Psi_k\rangle\langle\Psi_k|$, we let $\rho = |0^n\rangle\langle 0^n| \otimes \rho_B$, and let the superoperator Λ be defined as

$$\rho \mapsto \frac{1}{M} \sum_{w=0}^{M-1} \Lambda_w \rho \Lambda_w^\dagger \qquad (19)$$

where $\Lambda_w = (\mathcal{F} \otimes \mathcal{I})(\mathcal{I} \otimes \mathcal{U}_w)\mathcal{U}_f(\mathcal{I} \otimes \mathcal{U}_w)\mathcal{U}_f(\mathcal{F} \otimes \mathcal{I})$. Then the superoperator Λ can perform the period-finding algorithm efficiently without any initialization on the auxiliary qubits, since the probability of obtaining $|y\rangle$ satisfying (12) is

$$\mathrm{tr}\,[(|y\rangle\langle y| \otimes \mathcal{I})\Lambda(\rho)] = \frac{1}{N^2} \sum_{x=0}^{T-1} \left| \sum_{j=0}^{A_x} e^{2\pi i y j T/N} \right|^2, \quad (20)$$

which is the same probability as that of the original period-finding algorithm in (11). Furthermore, as in the initialization-free Simon algorithm, the resulting state after the measurement becomes $|y\rangle\langle y| \otimes \rho_B$ when y is the measurement outcome. Therefore, there exists an initialization-free quantum algorithm which can efficiently solve the period-finding problem.

In conclusion, we have investigated the initialization-free quantum algorithms, which do not require any initialization of the auxiliary qubits involved in the process of functional evaluation, and which recover the initial state of the auxiliary qubits after completing the computations. We have considered quantum algorithms for the Simon problem and the period-finding problem, and have presented the initialization-free quantum algorithms for the problems, which are as efficient as the original ones.

The iterative algorithms such as the Simon algorithm and the period-finding algorithm demand the storage of auxiliary qubits and the extra operations to initialize the state of the auxiliary qubits, whenever the procedure repeats. However if one utilizes our initialization-free technique then the size of the storage can be reduced and the extra operations can be omitted, since the same auxiliary qubits can repeatedly be used in our algorithms. Furthermore, since most known applications of the QFT can be considered as a generalization of finding unknown period of a periodic function (for example, Shor's factoring algorithm [5] and Hallgren's more recent algorithm for solving Pell's equation [10]), the initialization-free technique could be applied to a lot of implementations of quantum algorithms.

The authors would like to thank D. A. Lidar and M. Grassl for helpful comments. D.P.C. was supported by a Korea Research Foundation Grant (KRF-2004-059-C00060) and by Asian Office of Aerospace Research and Development (AOARD-04-4003).

[1] D. Deutsch, Proc. R. Soc. A **400**, 97 (1985); D. Deutsch and R. Jozsa, Proc. R. Soc. A **439**, 553 (1992).

[2] A. Berthiaume and G. Brassard, J. Mod. Optic. **41**, 2521 (1994).

[3] E. Bernstein and U. Vazirani, SIAM J. Comput. **26**, 1411 (1997).

[4] D. R. Simon, SIAM J. Comput. **26**, 1474 (1997).

[5] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).

[6] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[7] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, Fortschritte der Physik **46**, 493 (1998).

[8] C. H. Bennette, E. Bernstein, G. Brassard, and U. Vazirani, SIAM J. Comput. **26**, 1510 (1997).

[9] G. Brassard and P. Høyer, quant-ph/9704027, 1997.

[10] S. Hallgren, Proceedings of the thiry-fourth annual ACM Symposium on Theory of Computing, 2002, pp. 653–658; R. Jozsa, quant-ph/0302134, 2003.

[11] D. Biron, O. Biham, E. Biham, M. Grassl, and D. A. Lidar, Lecture Notes in Computer Science (Springer-Velag, Berlin, 1998) **1509**, 140 (1999); E. Biham, O. Biham, D. Biron, M. Grassl, and D. A. Lidar, Phys. Rev. A **60**, 2742 (1999); E. Biham, O. Biham, D. Biron, M. Grassl, D. A. Lidar, and D. Shapira, Phys. Rev. A **63**, 012310 (2000).

[12] E. Biham and D. Kenigsberg, Phys. Rev. A **66**, 062301 (2002).

[13] S. Parker and M. B. Plenio, Phys. Rev. Lett. **85**, 3049 (2000).

[14] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).

[15] D. P. Chi, J. Kim, and S. Lee, J. Phys. A **34**, 5251 (2001); J. Kim, S. Lee, and D. P. Chi, J. Phys. A **35**, 6911 (2002).